

CLAIMS

1. A remote terminal in a wireless communication system, comprising:
- 2 a data processing unit configured to process data for a communication over a wireless link;
- 4 a main processor coupled to the data processing unit and configured to provide control for the remote terminal, wherein the data processing unit and main processor are
- 6 unsecured units vulnerable to being spoofed by external entities; and
- 8 a secure unit operatively coupled to the main processor and including
- 10 a secure processor configured to perform secure processing for the remote terminal, and
- 12 a secure memory configured to provide secure storage of data, and wherein the secure unit is physically encapsulated within a secure module and further configured to prevent unauthorized accesses to the secure memory via hardcoded protocols.
2. The remote terminal of claim 1, wherein the secure unit further includes
- 2 a read only memory (ROM) configured to store program instructions and parameters used for the secure processing.
3. The remote terminal of claim 2, wherein the ROM is embedded within
- 2 the secure processor.
4. The remote terminal of claim 1, wherein the secure processor and secure
- 2 memory are implemented and physically encapsulated within a single integrated circuit (IC).
5. The remote terminal of claim 1, wherein the secure processor and secure
- 2 memory are physically encapsulated within a tamper resistance or tamper evident unit.
6. The remote terminal of claim 1, wherein the secure processor and secure
- 2 memory are permanently affixed within the remote terminal.

7. The remote terminal of claim 1, wherein messaging and data are
2 exchanged with the secure unit via a single entry point provided by a bus.

8. The remote terminal of claim 1, wherein the secure unit is configured to
2 implement public-key cryptography for the secure processing.

9. The remote terminal of claim 8, wherein a private key assigned to the
2 remote terminal is embedded within the secure processor.

10. The remote terminal of claim 9, wherein the private key is permanently
2 etched within the secure processor.

11. The remote terminal of claim 9, wherein the private key assigned to the
2 remote terminal is stored in a ROM within the secure processor.

12. The remote terminal of claim 1, wherein the secure processor is
2 configurable to implement one or more security protocols.

13. The remote terminal of claim 12, wherein the one or more security
2 protocols include Secure Sockets Layer (SSL) protocol or Transport Layer Security (TLS) protocol, or both.

14. The remote terminal of claim 1, wherein the secure unit is configurable
2 to act in a role of a client or a server for each secure transaction with a foreign entity.

15. The remote terminal of claim 1, wherein the secure memory is
2 configured to store electronics funds.

16. The remote terminal of claim 1, wherein the secure memory is
2 configured to store cryptographic parameters used for the secure processing.

17. The remote terminal of claim 1, wherein the secure memory is
2 configured to store one or more certificates used for authentication.

18. The remote terminal of claim 17, wherein a certificate is loaded into the
2 secure memory via a secure transaction with a certificate authority.

19. The remote terminal of claim 18, wherein different levels of security is
2 implemented for a certificate loading transaction depending on whether or not a
certificate has already been loaded to the remote terminal.

20. A remote terminal in a wireless communication system, comprising:
2 a data processing unit configured to process data for a communication over a
wireless link;
4 a main processor coupled to the data processing unit and configured to provide
control for the remote terminal, wherein the data processing unit and main processor are
6 unsecured units vulnerable to being spoofed by external entities; and
a secure unit embedded within the main processor and configured to perform
8 secure processing for the remote terminal and provide secure storage of data, wherein
the secure unit is further configured to implement public-key cryptography for the
10 secure processing, and wherein the secure unit is further configured to prevents
unauthorized accesses to securely stored data via hardcoded protocols.

21. A method for providing secure processing and data storage for a wireless
2 communication device, comprising:
defining a secure processor within the communication device for performing
4 secure processing;
defining a secure storage within the communication device for providing secure
6 data storage;
storing program instructions and parameters used for the secure processing
8 within the secure processor or secure storage, wherein the stored program instructions
implement hardcoded protocols; and
10 physically encapsulating the secure processor and secure storage within a secure
unit.

22. The method of claim 21, wherein the secure processor and secure storage
2 are physically encapsulated within a single integrated circuit (IC).

23. The method of claim 21, further comprising:
2 permanently affixing the encapsulated secure processor and secure storage
within the communication device.

24. A method for providing secure processing and data storage for a wireless
2 communication device, comprising:

receiving a first message to initiate a secure transaction with a foreign entity;
4 authenticating the foreign entity through a secure processor located within the
communication device; and
6 if the foreign entity is authenticated, performing securing processing for the
secure transaction through the secure processor, and
8 wherein the secure unit is physically encapsulated within a secure module and
further configured to prevents unauthorized accesses to the secure memory via
10 hardcoded protocols.

25. The method of claim 24, wherein the secure processing is performed
2 based on program instructions stored within the secure processor.

26. The method of claim 24, wherein the authentication is achieved via
2 exchanges of certificates.